(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3633953 A1**

(51) Int. Cl.⁴:
G05B 9/03
F23N 5/20
F23N 5/24
// G06F 15/46

(21) Aktenzeichen: P 36 33 953.9
(22) Anmeldetag: 6. 10. 86
(43) Offenlegungstag: 7. 4. 88

DE 3633953 A1

(71) Anmelder:
Siemens AG, 1000 Berlin und 8000 München, DE

(72) Erfinder:
Daar, Horst, Dr.-Ing., 8520 Erlangen, DE; Mark, Reinhard, Dipl.-Ing., 8459 Hirschberg, DE; Schütz, Hartmut, Dipl.-Ing., 8551 Heroldsbach, DE; Wenzinger, Martin, Dipl.-Phys., 8520 Erlangen, DE

(54) Verfahren zum Betrieb eines programmgesteuerten Automatisierungsgeräts

Für ein programmgesteuertes, redundant mit zwei Teilsystemen (AB) aufgebautes sicherheitsgerichtetes Automatisierungsgerät (AG) wird vorgeschlagen, zwei identische Programmabläufe vorzusehen und vom Betriebssystem (BS) zu Beginn bestimmter Programmabschnitte eine gegenseitige Synchronisation der Programmabläufe durchzuführen. Diese Synchronisation ist auch vom Anwenderprogramm an beliebigen Programmpunkten aufrufbar. Das Betriebssystem streut ferner zur Minimierung der Prozessorbelastung die einzelnen Elemente eines Selbsttests in Abhängigkeit von der momentanen Prozeßbelastung in den Programmablauf ein.

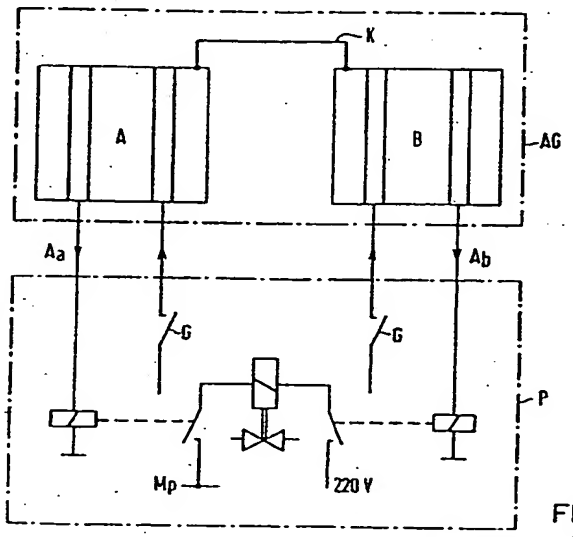

FIG 1

DE 3633953 A1

SDOCID: <DE_____3633953A1_I_>

Patentansprüche

1. Verfahren zum Betrieb eines programmgesteuerten, redundant mit zwei Teilsystemen aufgebauten Automatisierungsgeräts für einen technischen Prozeß, insbesondere für eine Brenneranlage, **dadurch gekennzeichnet**, daß zwei identische Programmabläufe vorgesehen sind und das Betriebssystem zu Beginn bestimmter Programmabschnitte eine gegenseitige Synchronisation der Programmabläufe vornimmt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die die gegenseitige Synchronisation vornehmende Synchronisation der Programmabläufe der beiden Teilsysteme *(A, B)* vom Anwenderprogramm an beliebigen Programmpunkten aufrufbar ist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein Selbsttest in einzelne Selbsttestelemente aufgeteilt und vom Betriebssystem in Abhängigkeit von der momentanen Prozessorbelastung in den Programmablauf eingestreut werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß vom Betriebssystem bei Auftreten eines Fehlers in einem Teilprozeß dieser passiviert und ohne in den Stopp-Zustand zu gehen ein entsprechender Ersatz-Teilprozeß zugeschaltet wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei Ungleichheit redundanter Eingangssignale vom Betriebssystem eine Unterscheidung zwischen laufzeitbedingten Signaldiskrepanzen und echten Fehlern durchgeführt wird, wobei die Diskrepanzzeiten vom Anwenderprogramm parametrierbar sind.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Betriebssystem zur Behandlung ein- oder zweikanalig ausgeführter Prozeßperipherie eingerichtet ist.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß für den Sicherheitsbetrieb das Anwenderprogramm in einen nicht flüchtigen Speicher geladen wird und das Betriebssystem zur Erkennung dieses Speichermediums eingerichtet ist und damit zwischen Test- und Sicherheitsbetrieb unterscheiden kann.

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Betrieb eines programmgesteuerten Automatisierungsgeräts gemäß dem Oberbegriff des Anspruchs 1.

Aufgabe der Erfindung ist es, ein Verfahren anzugeben, mit dem ein derartiges Gerät sicher und von der Anwenderseite gesehen flexibel und mit großer Verfügbarkeit betrieben werden kann.

Diese Aufgabe wird erfindungsgemäß durch die im Kennzeichen des Anspruchs 1 angegebenen Merkmale gelöst.

Weitere Ausgestaltungen der Erfindung, welche nachfolgend anhand der Figuren näher erläutert werden, sind Gegenstände der Unteransprüche.

Fig. 1 zeigt ein zweikanalig redundant aufgebautes sicherheitsgerichtetes Automatisierungsgerät *AG*, mit seinen Teilsystemen *A* und *B*, welches einen technischen Prozeß *P*, beispielsweise eine Ölbrenneranlage mit den Ausgangssignalen A_a und A_b steuert. Geber *G* liefern die Eingangssignale E_a und E_b für das Automatisierungsgerät. Die Teilsysteme *A* und *B* arbeiten stets mit identischen Programmen und synchronisieren sich über eine Rechnerkopplung, welche mit *K* angedeutet ist.

Redundante Automatisierungsgeräte erfordern eine Synchronisation der Teilgeräte. Bisher bekannte Geräte synchronisieren sich nach einem starren Zeitraster, z. B. taktsynchron, befehlssynchron oder per Software, in größeren Zeitabständen. Bei der Erfindung hingegen wird ein flexibler Mittelweg gewählt, derart, daß das Synchronisationsraster an jeden Anwendungsfall anpaßbar ist, indem vom Betriebssystem ein minimales Synchronisationsraster vorgegeben wird (**Fig. 3**), das der Anwender durch Aufruf von Betriebssystemfunktionen beliebig verfeinern kann. Dadurch kann beispielsweise die maximale Alarmreaktionszeit begrenzt werden. Der Vorteil dieses Verfahrens liegt darin, daß einerseits unnötige Synchronisationen, die eine zeitliche Belastung des Prozessors bedeuten können, vermieden werden und andererseits keine Spezialkomponenten (Vergleicher) benötigt werden.

Oft wird für zweikanalige, sicherheitsgerichtete Automatisierungsgeräte ein Selbsttest des Geräts im laufenden Betrieb gefordert, um durch Offenbarung von Fehlfunktionen Schaden für Personen und Umwelt zu verhindern. Die Laufzeit der Selbsttestroutinen liegt im Minutenbereich. Die Testzykluszeit, d. h. die Zeit innerhalb der ein Selbsttest vollständig durchlaufen sein muß, ist abhängig vom Anwendungsfall, z. B. Bergseilbahnen, Brennersteuerungen. In herkömmlicher Weise wird hierzu das gesamte Selbsttestprogramm in Scheiben unterteilt und diese in einer starren Folge bearbeitet. Dies führt zu einem unnötig häufigen Selbsttest, da die Größe der Testscheibe nach der ungünstigsten Prozessorbelastung ausgelegt werden muß.

Mit der Erfindung wird dagegen die Testscheibenmenge selbsttätig optimiert. In Abhängigkeit von der momentanen Prozessorbelastung bestimmt der Selbsttestmanager des Betriebssystems *BS* — siehe **Fig. 3** — die Anzahl der zu aktivierenden Testscheiben. Der Vorteil dieses Verfahrens besteht in der Minimierung der Prozessorbelastung durch Selbsttest und damit Erhöhung der Nutzleistung des Geräts.

Die Normalreaktion eines zweikanaligen Sicherheitssystems bei Auftreten eines Fehlers ist der Übergang in die "sichere Ruhelage", d. h. Stopp des gesamten Automatisierungssystems. Im Interesse einer möglichst hohen Anlagenverfügbarkeit wird bei der Erfindung statt dessen bei Auftreten eines Peripheriefehlers der betreffende Teilprozeß von den Teilprozessen $TP_1 - TP_n$ (**Fig. 2**) des Prozesses passiviert und ein entsprechender Ersatz-Teilprozeß aktiviert. Beispiel: Steuerung mehrerer Ölbrenner für einen Dampfkessel. Ein sicherheitsgerichtetes Automatisierungsgerät steuert mehrere Ölbrenner eines Dampfkessels. Jeder Brenner stellt, mit seinen Ein- und Ausgangssignalen einen Teilprozeß dar. Die oben genannte Normalreaktion würde, bei Auftreten eines einzigen Fehlers, z. B. in einer Peripheriebaugruppe, zur Stillsetzung aller von diesem Automatisierungsgerät gesteuerten Ölbrenner führen. Bei Verwendung des erfindungsgemäßen Verfahrens wird dagegen nur der betroffene Ölbrenner durch das Betriebssystem sicherheitstechnisch isoliert und ein Ersatzbrenner zugeschaltet. Der Gesamtprozeß (Dampfkessel) läuft ungestört weiter.

Ziel einer Prozeßsignalredundierung ist es, Peripheriefehler mittels Signalvergleich zu erkennen. Einbau- oder Bauteiltoleranzen führen in der Regel dazu, daß redundante Eingangssignale sich nicht zeitgleich verän-

dern (Beispiel: Zwei getrennte Endschalter). Die Berücksichtigung derartiger Signallaufzeitunterschiede oblag bisher dem Anwender. Das Sicherheitsrisiko, bedingt durch Programmierfehler wird dadurch erhöht.

Mit dem erfindungsgemäßen Verfahren erfolgt dagegen die Unterscheidung zwischen zulässigen zeitlichen Signaldiskrepanzen und echten Peripheriefehlern durch das Betriebssystem. Statt Programmierung wird die maximal zulässige Diskrepanzzeit jedes Eingangssignals dem Betriebssystem per Projektierung mitgeteilt (Parametrierung) und auf Plausibilität geprüft. Die Wahrscheinlichkeit eines Anwenderfehlers wird dadurch deutlich erniedrigt und der Programmieraufwand vermindert.

Häufig sind nicht alle Prozeßsignale sicherheitsrelevant. Diese können einkanalig am Automatisierungsgerät aufgelegt werden. Bekannte zweckmäßige Automatisierungssysteme lassen eine Mischung von zwei- und einkanaliger Peripherie, wie es die Erfindung vorsieht, in einem Gerät nicht zu. Bei dem erfindungsgemäßen Verfahren wird dem Betriebssystem per Parametrierung der Signaltyp (ein- oder zweikanalig) mitgeteilt. Das Betriebssystem behandelt die Prozeßsignale entsprechend ihrem Typ und verteilt alle Eingangssignale an die Teilsysteme.

Aus sicherheitstechnischen Gründen sind die Eingriffmöglichkeiten in laufende Geräte stark eingeschränkt. So ist das Ändern von Daten und Befehlen beim Sicherheitsbetrieb unzulässig. Derartige Hilfsmittel sind aber zur Inbetriebsetzung und zu Testzwecken unerläßlich.

Die Erfindung sieht vor, das Betriebssystem zur selbsttätigen Unterscheidung zwischen Test- und Sicherheitsbetrieb zu ertüchtigen. Der Vorteil ist eine kürzere Inbetriebsetzungsdauer.

Es wird hierzu der Typ des im Gerät gesteckten Anwenderprogrammspeichers ausgenutzt: Sicherheitsbetrieb liegt immer dann vor, wenn das Anwenderprogramm in einem nicht flüchtigen Speicher (EPROM) geladen ist. Das Betriebssystem wird nun erfindungsgemäß dazu eingerichtet, daß es den Speichertyp der Quelle des Anwenderprogramms erkennt und somit das den Sicherheitsbetrieb steuernde Anwenderprogramm von den für Testzwecke bestimmten Programmen, welche in flüchtige Speicher (RAM) geladen werden, unterscheiden kann.

– Leerseite –

3633953

Nummer: 36 33 953
Int. Cl.4: G 05 B 9/03
Anmeldetag: 6. Oktober 1986
Offenlegungstag: 7. April 1988

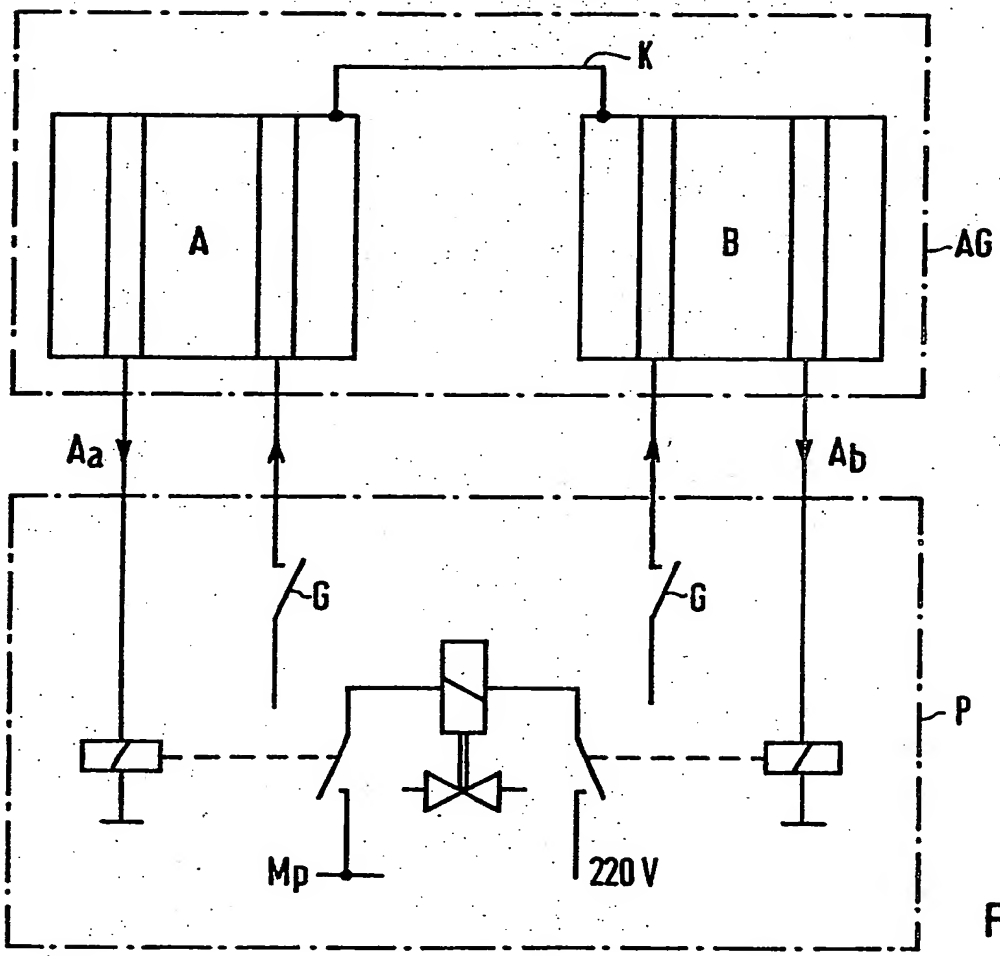

FIG 1

FIG 2

NACHGEREICHT

Programmablauf

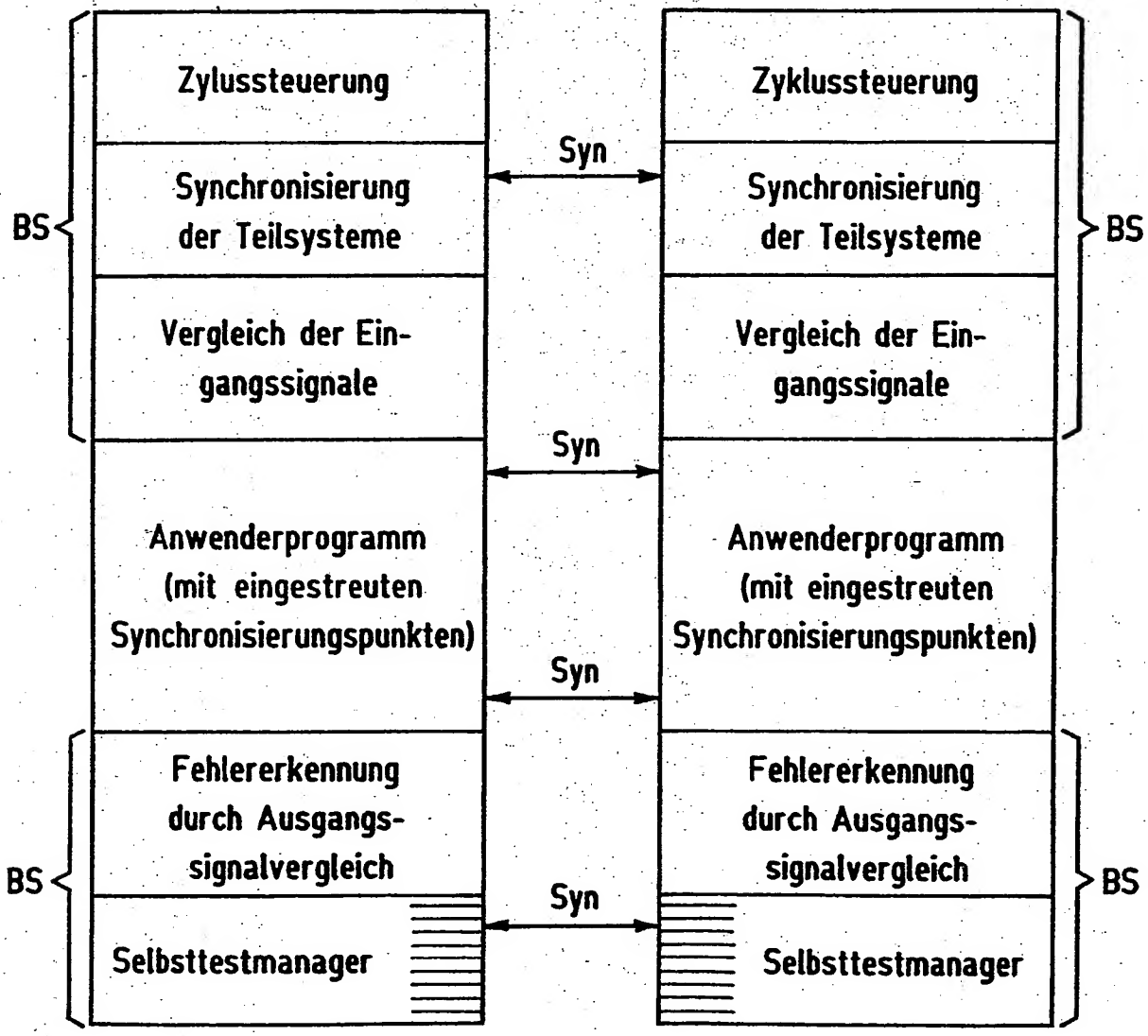

FIG 3